WHAT IS CLAIMED IS:

  1. A method for activating a wireless network security with a wireless host, comprising:

5 establishing a communication connection with a client;

  in response to the communication connection, automatically requesting from the client a determination of whether to activate the wireless network security;

10 upon receipt of the determination to activate the wireless security network, automatically requesting an identifier code from the client; and 52

  activating the wireless security network to secure the wireless host if the identifier code matches a unique

15 key-code that is physically located on the wireless host.

  2. The method of Claim 1, further comprising registering the client with the wireless host such that the wireless host is able to identify the client upon

20 subsequent connections.

  3. The method of Claim 1, further comprising saving the configuration setting on the client as part of a profile or a service set identifier (SSID) such that

25 access to the wireless host is maintained.

  4. The method of Claim 1, further comprising following the activation of the wireless security network, changing the unique key-code to a personal code

30 selected by the client.

5.   The method of Claim 4, further comprising resetting the unique key-code to a factory default.

5   6.   The method of Claim 1, further comprising, in response to the determination of not to activate the wireless network security, setting a reminder flag.

7.   The method of Claim 6, wherein the remainder flag comprises a reminder time period such that a second request is made from the client for the determination to activate the wireless security network after the expiration of the reminder time period.

8.   The method of Claim 6, wherein the reminder flag comprises a reminder condition such that a second request is made from the client for the determination to activate the wireless security network upon a subsequent communication connection.

9.   The method of Claim 6, wherein the reminder flag comprises a never-reminder response.

10.   The method of Claim 6, further comprising registering the client to save configuration information on the client such that the wireless host recognizes the client on a subsequent communication connection.

11.   A method of accessing a secured wireless
network deployed from a wireless router using a client,
comprising:

establishing a communication connection with a

5   client;

in response to the communication connection,
automatically requesting from the client an identifier
code to access the secured wireless network; and

allowing access to the secured wireless network on

10   the wireless router if the identifier code matches a
unique key-code that is physically located on the
wireless router.

12.   The method of Claim 11, further comprising

15   denying access to the secured wireless network if the
identifier code supplied by the client does not match the
unique key-code.

13.   The method of Claim 12, further comprising, in

20   response to denying access to the secured wireless
network, disassociating the communication connection with
the wireless router.

14.   The method of Claim 11, further comprising, in

25   response to allowing access to the secured wireless
network, changing the unique key-code that is physically
located on the wireless router to a personal code
supplied by the client.

15. The method of Claim 10, further comprising registering the client with the wireless router such that the wireless router is able to identify the client upon subsequent connections.

5

16. The method of Claim 10, further comprising saving the configuration setting on the client as part of a profile or a service set identifier (SSID) such that access to the wireless host is maintained.

10

17. A system for deploying a wireless network security with a wireless router, comprising:

a wireless router having a unique key-code physically located on the router;

5   a client operably maintains a communication connection with the router, the client operable to activate a wireless security network to secure the router if the client transmits an identifier code to the router wherein the identifier code matches a unique key-code

10   that is physically located on the router.

18. The system of Claim 17, wherein the unique key code is a service tag supplied with the router.

15   19. The system of Claim 17, wherein the unique key code is a local area network (LAN) media access control (MAC) address supplied with the router.

20. The system of Claim 17, wherein the client is

20   an information handling system.